



Chip-Backside Vulnerability to Intentional Electromagnetic Interference in Integrated Circuits

Wadatsumi, Takuya ; Monta, Kazuki ; Hayashi, Yusuke ; Miki, Takuji ; Hatzopoulos, Alkis A. ; Barić, Adrijan ; Nagata, Makoto

(Citation)

IEEE Transactions on Electromagnetic Compatibility, 66(5):1556-1566

(Issue Date)

2024-10

(Resource Type)

journal article

(Version)

Version of Record

(Rights)

© 2024 The Authors.








This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License

(URL)

<https://hdl.handle.net/20.500.14094/0100491864>



Chip-Backside Vulnerability to Intentional Electromagnetic Interference in Integrated Circuits

Takuya Wadatsumi , *Student Member, IEEE*, Kazuki Monta , *Member, IEEE*, Yusuke Hayashi ,
 Takuji Miki , *Member, IEEE*, Alkis A. Hatzopoulos , *Life Senior Member, IEEE*,
 Adrijan Barić , *Senior Member, IEEE*, and Makoto Nagata , *Senior Member, IEEE*

Abstract—The backside of integrated circuits (ICs) in flip-chip assembly is susceptible to intentional electromagnetic interference due to its open surface. In this article, we propose a model in which conducted current noise from a localized area of the Si substrate on the chip-backside causes errors in complementary metal-oxide-semiconductor (CMOS) digital circuits. This model explains for the first time the mechanism of bit-flip errors in bistable circuits caused by high-voltage pulse (HVP) injection on the backside of the IC. The injected current from the backside of the IC not only flows into the power distribution network, but also charges the gate capacitance of the next stage via p–n junction diodes of body/drain or body/source in N-channel MOSFETs (NMOS) with twin-well structures, resulting in bit-flip errors. In this study, circuit simulations were performed using a three-dimensional RC network model of the IC chip and an HVP injector. These simulations have shown that the P-well voltage is biased depending on the arrangement of the tap cells, reproducing bit-flip errors in the bistable circuit of a D flip-flop. The simulation results were validated on a fabricated prototype IC chip, which confirmed the trend of data dependency for errors related to the physical layout.

Index Terms—Bit-flip, fault injection, flip-chip assembly, intentional electromagnetic interference (IEMI), integrated circuits (ICs), soft error.

I. INTRODUCTION

THE safety and reliability of electrical and electronic systems in the electromagnetic environment are critical, as electromagnetic interference can cause logical errors and device faults. Mission-critical systems, such as connected cars, robots, and large-scale servers, are at increased risk of malicious intentional electromagnetic interference (IEMI) attacks due to

their valuable resources [1], [2], [3]. Unlike a hacking attack via the network, the signs of an IEMI attack are difficult to detect and often only become apparent when the system stops working properly.

An IEMI risk assessment is systematized according to the need for the following [4]:

- 1) access to areas;
- 2) access to knowledge;
- 3) access to financial resources.

In situations where access to areas is critical, attackers can bypass physical barriers and attack devices directly. In attacks executed through a higher level of knowledge required to carry out the attack, the attacker, who has a deep understanding of semiconductor and system architectures as well as the intricacies of attack injection methods, can strategically target specific locations and timings within the integrated circuit (IC). In addition, there are attacks that require a high level of financial resources by large organizations, such as national research institutes and enterprise companies.

Commercially available electronic devices usually follow strict standards for electromagnetic compatibility (EMC) and reliability to ensure a certain level of disturbance tolerance [5], [6]. However, these standards are intended to assess immunity to unexpected interference that may occur in the real-world environment, which limits the frequency, intensity, and propagation path. Therefore, discussions on malicious IEMI aimed at the loss of functionality of electronic systems or the acquisition of confidential information in semiconductors must be separated from EMC standards [7].

IEMI on ICs has been demonstrated as contactless or near-field attacks in [8], [9], [10], and [11] to derive confidential information by intentionally altering the operation of circuits. In contrast, this article deals with direct interference attacks [12], [13], [14], [15] on ICs, where access to the ICs is possible and a high level of knowledge is required to perform the attack. In particular, the backside of the Si substrate of flip-chip mounted ICs, which is favored for high performance ICs with a large number of input/outputs (I/Os), is vulnerable to interference [12], [13], [14], [15]. This vulnerability is due to the fact that the chip-backside is usually open and, thus, susceptible to localized attacks, while the chip surface is less vulnerable due to the metal wires created by the back end of line process. Even if the complementary metal-oxide-semiconductor (CMOS) layout is not normally visible from the backside, it can

Manuscript received 27 March 2024; revised 14 July 2024; accepted 3 August 2024. Date of publication 28 August 2024; date of current version 28 October 2024. This work was supported in part by JSPS KAKENHI under Grant JP22H04999, in part by the SECOM Science and Technology Foundation, and in part by the JSPS Overseas Challenge Program for Young Researchers. (Corresponding author: Takuya Wadatsumi.)

Takuya Wadatsumi, Kazuki Monta, Yusuke Hayashi, Takuji Miki, and Makoto Nagata are with the Graduate School of Science, Technology and Innovation, Kobe University, Kobe 657-8501, Japan (e-mail: takuya.wadatsumi@it1.stin.kobe-u.ac.jp; kazuki.monta@it1.stin.kobe-u.ac.jp; yusuke.hayashi@it1.stin.kobe-u.ac.jp; miki@port.kobe-u.ac.jp; nagata@cs.kobe-u.ac.jp).

Alkis A. Hatzopoulos is with the Electronics Laboratory, Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Thessaloniki 54124, Greece (e-mail: alkis@ece.auth.gr).

Adrijan Barić is with the Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb 10000, Croatia (e-mail: adrijan.baric@fer.hr).

Color versions of one or more figures in this article are available at <https://doi.org/10.1109/TEMC.2024.3440919>.

Digital Object Identifier 10.1109/TEMC.2024.3440919

be made visible with the aid of an infrared microscope. Chip encapsulation methods also contribute to this vulnerability. In wire-bond mounting, the chip surface contains circuits where the wire bonds are connected and they are all encapsulated in resin to reduce the risk of damage. Flip-chip assembly, on the other hand, uses thin resin or metal covers for efficient heat dissipation, as there is no circuitry on the backside that is exposed to the outside. Therefore, an attacker can easily remove the encapsulation material and gain access to any part of the backside of the IC by chemical or mechanical manipulation.

Circuit simulation for logical errors against disturbances from outside ICs is important to estimate device immunity and system response prior to IC fabrication and electronic device manufacturing. Simulation of the response to external disturbances entering electronic devices has been widely discussed in the areas of soft errors caused by cosmic rays, EMC, and electrostatic discharge (ESD). In each of these areas, different methods are used depending on the coupling path of the particular disturbance and the scope of the simulation.

Soft errors due to cosmic rays are caused by neutrons and α -rays reaching the Si substrate and creating electron-hole pairs near the p–n junction, which often leads to memory errors. This phenomenon is modeled by simulating the excited current at the device level [16], [17] and integrated into circuit models to account for error factors [18]. However, this approach is difficult to apply to the analysis of disturbance responses over a large area within a chip, as it analyzes the events for a single particle collision.

For EMC and ESD, the conductive and spatial coupling is modeled between standardized noise source and chassis or printed circuit board. The system is evaluated by connecting the coupling path model and an IC model [19], [20], [21], [22]. However, the direct coupling to the internal nodes of the ICs is normally not included in these simulation models.

In chip-level IEMI, the construction of models to analyze phenomena and develop countermeasures for fault injection into circuits intended for system shutdown or skipping is discussed [8], [9], [10], [11], [12], [13], [14], [15], [23]. However, the direct coupling to an IC chip is complex. Therefore, the construction of the model requires in-depth knowledge of device structure, circuit design, and measurement techniques. For this reason, the errors observed in measurements are often not explicitly clarified for potential mechanisms.

In this article, a new model for analyzing errors in static bistable circuits caused by IEMI attacks from the backside of the IC is developed and described in detail based on simulation and measurement results.

The rest of this article is organized as follows. Section II describes the mechanism of current propagation by high-voltage pulse (HVP) injection on the backside of ICs. Section III presents a circuit-level approach for the bit-flip phenomenon in bistable circuits in D flip-flop (D-FFs). Section IV describes a bit-flip error simulation for HVP injection from the backside of ICs, which includes the IC chip model that represents the propagation path and the HVP injector model that generates the surge voltage. In Section V, observations of bit-flip error by HVP injection are conducted on a prototype chip, and the experimental results

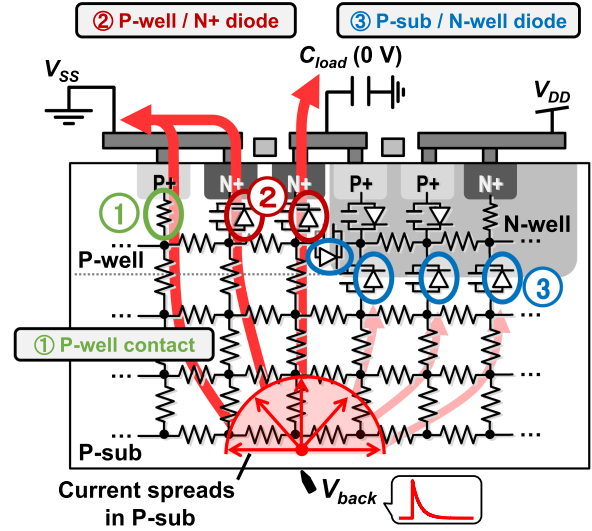


Fig. 1. Current path by HVP injection on the IC backside.

confirm the simulation model. Finally, Section VI concludes this article.

II. HVP INJECTION ON THE BACKSIDE OF ICs

In this article, the effects of the positive HVP injection from the backside of the bulk twin-well CMOS chip are analyzed in detail, as shown in Fig. 1. P-well and P-sub perform similar functions and the doping levels are similar but not identical. Therefore, P-well and P-sub are explicitly separated in this work.

The current caused by HVP injection on the backside of an IC propagates spatially through the resistive network forming the Si substrate. The area of influence on the CMOS circuit varies significantly with the Si substrate thickness, which has been confirmed by measurements and simulations [12], [15].

We hypothesize that the injected current flows through the following (see Fig. 1):

- ① P-well contact (primarily)
- ② P-well/N+ diode (possibly)
- ③ P-sub/N-well diode (possibly)

The path of current flow is related to the threshold voltage V_{th} of the p–n junction diode and the characteristics of the voltage waveform induced by HVP injection, such as the polarity and the intensity.

When the HVP injection is positive, P-sub and P-well are positively biased. Therefore, it is possible for current to flow through ② P-well/N+ diode and ③ P-sub/N-well diode. The P-well resistivity ρ_{well} is typically higher than the metal resistivity ρ_{metal} , so the P-well voltage between the well contacts on the left and right sides of Fig. 2 can vary significantly with distance from the well contacts. With an initially uncharged gate capacitance $C_{load} (0V)$ of the next stage, the P-well voltage exceeding V_{th} allows the current to flow through the ② P-well/N+ diode. In contrast, ③ P-sub/N-well diode requires the voltage $V_{th} + V_{DD}$ of the P-sub for current to flow, since N-well is biased at V_{DD} . Therefore, with the positive HVP injection, the current tends to flow in the order ① → ② → ③, according to its voltage amplitude.

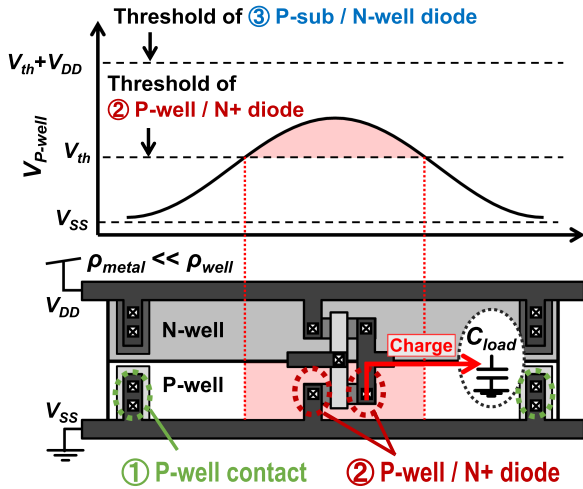


Fig. 2. Description P-well/N+ diode.

When the HVP injection is negative, P-sub and P-well are negatively biased. Therefore, no current flows at the p–n junction diode at ②P-well/N+ diode and ③P-sub/N-well diode. The current flow is limited to ①P-well contact.

Chancel et al. [15] have proposed an IC chip model for HVP injection on the backside of the IC that includes only paths ①P-well contact and ③P-sub/N-well diode. Because of their focus on the circuit errors caused by unwanted timing delays, the paths ① and ③ were only considered. The circuit delays occur due to $V_{DD} - V_{SS}$ fluctuations, the so-called current resistance drops. During the positive HVP injection, the current flows to ① and ③, causing the V_{DD} and V_{SS} fluctuations to cancel each other out. However, with the negative HVP injection, the current only flows to ①, resulting in a large fluctuation only at V_{SS} . Therefore, they have concluded that the negative voltage injection from the backside of the chip causes errors more efficiently than the positive voltage injection.

In contrast, we have experimentally observed the bit-flips in static bistable circuits due to the positive HVP injection [13]. This error cannot be explained by the model of Chancel et al. [15].

In this article, we propose an IC chip model for the bit-flips in static bistable circuits caused by a positive pulse that charges the gate capacitance C_{load} in the next stage. This model contains paths ①P-well contact, ②P-well/N+ diode, and ③P-sub/N-well diode as well as the resistivity of the silicon substrate and the metal layer, and the capacitance between the well layers. The mechanism of bit-flip in bistable circuits by charging C_{load} is described in detail in Section III.

III. BIT-FLIP MECHANISM IN CIRCUIT LEVEL

In this section, the mechanism of bit-flip in bistable elements caused by voltage injection from the backside of the chip is explained using simulation program with integrated circuit emphasis (SPICE) where a D-FF is modeled in a schematic netlist at transistor-level. The current injected by the HVP injection propagates through the resistor network representing the Si substrate.

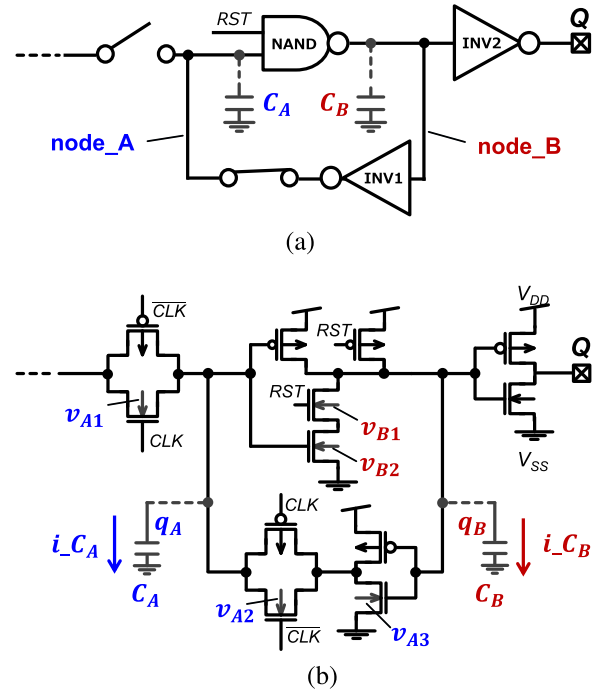


Fig. 3. Schematic and functional explanation of the follower section in a D-FF for bit-flip. (a) Logic-level schematic. (b) Transistor-level schematic.

Almost all of the current flows through well contacts near the HVP injection position to the power distribution network (PDN). The P-well voltage fluctuates locally between the well contacts. Therefore, the p–n junction diodes between P-well and N+ drain or P-well and N+ source of the N-channel MOSFETs (NMOS) transistors have chances to become conductive and subsequently the gate capacitance of the next stage is charged. As a result, the state of the bistable elements may be inverted. The static state of the D-FF is impacted, more precisely, the state in which the value is latched in the follower part of the D-FF gets upset.

An abstracted diagram of circuit of the follower part of the D-FF with latched value is shown in Fig. 3(a). A detailed circuit is shown in Fig. 3(b). This circuit is a typical D-FF with asynchronous reset. C_A and C_B represent the total capacitances associated with node_A and node_B, respectively. The charge on each capacitance at node_A and node_B is defined as q_A and q_B . The voltages applied to the bodies of the NMOS transistors by HVP injection are $v_A = [v_{A1}, v_{A2}, v_{A3}]$ and $v_B = [v_{B1}, v_{B2}]$, and these voltages cause the currents i_{C_A} and i_{C_B} to flow to node_A and node_B, respectively. For simplicity, in this Section III, a test pulse with the voltage amplitude of V_{pA} is applied to v_{A1} , v_{A2} , and v_{A3} . Similarly, a test pulse with the voltage amplitude of V_{pB} is applied to v_{B1} and v_{B2} . When the Q terminal asserts “0,” q_A is uncharged and q_B is fully charged. When the Q terminal asserts “1,” q_A is fully charged and q_B is uncharged. The change of the output Q from “0” to “1” is defined as “bit-set error” and from “1” to “0” as “bit-reset error” during HVP injection.

Fig. 4 shows that the distribution of bit-flip events when the voltages of V_{pA} and V_{pB} are comprehensively scanned from low (0 V) to high (2 V). Fig. 4(a) and (b) is for the cases where

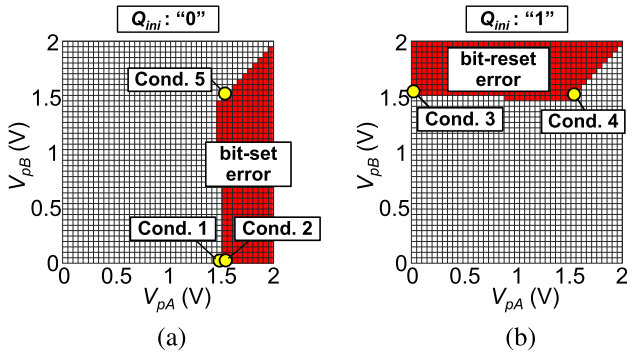


Fig. 4. Color maps of bit-flip error. (a) Bit-set error. (b) Bit-reset error.

TABLE I
BIT-FLIP CIRCUIT SIMULATION RESULTS

Cond.	V_{pA} (V)	V_{pB} (V)	Q_{ini}	Results
1	1.5	0	"0"	no change
2	1.55	0	"0"	bit-set error
3	0	1.55	"1"	bit-reset error
4	1.55	1.55	"1"	bit-reset error
5	1.55	1.55	"0"	no change

Q initially asserts "0" or "1," respectively. These results show that the occurrence of "bit-set error" and "bit-reset error" is characterized by the initial state of Q , as Q_{ini} and the injected pulse amplitudes V_{pA} and V_{pB} .

The parameters and results for each of the five conditions under HVP injection are summarized in Table I, and the corresponding waveforms are shown in Fig. 5. The symbols q_{thA} and q_{thB} represent the threshold charges at node_A and node_B, respectively in Fig. 3, which are the total charges q_A and q_B required to invert the output states of the 2-input NAND logic gate (NAND) and the inverter (INV1).

In Cond. 1, i_{C_A} , which flows from the P-well body, charges C_A . However, since the accumulated charge q_A is not larger than q_{thA} , it is not sufficient to invert the output of the NAND. Consequently, the current and charge are released on the falling edge of the pulse and a "no change" takes place.

In Cond. 2, the process leads to the "bit-set error." At the beginning, C_A is gradually charged. As soon as q_A exceeds the threshold charge q_{thA} , NAND starts to change its state and the output charge q_B starts to discharge at t_1 . Then, q_B gradually discharges, causing q_B to fall below the threshold q_{thB} at t_2 .

In Cond. 3, the "bit-reset error" occurs. The process follows a similar mechanism as in Cond. 2. First, C_B is gradually charged. As soon as q_B exceeds the threshold charge q_{thB} , INV1 starts to change its state and the output charge q_A starts to discharge at t_1 . Then, q_A gradually discharges, causing q_A to fall below the threshold q_{thA} at t_2 .

Under Cond. 4 and Cond. 5, the same amplitude is applied to v_A and v_B , but starting from different initial values Q_{ini} . In both scenarios, q_A and q_B remain above their respective threshold q_{thA} and q_{thB} during the pulse injection period ($t_1 < t < t_2$). As a result, INV1 and NAND output low state, resulting in a discharge at q_A and q_B as soon as the pulse falls. However, since the capacitance C_A is smaller than the capacitance C_B

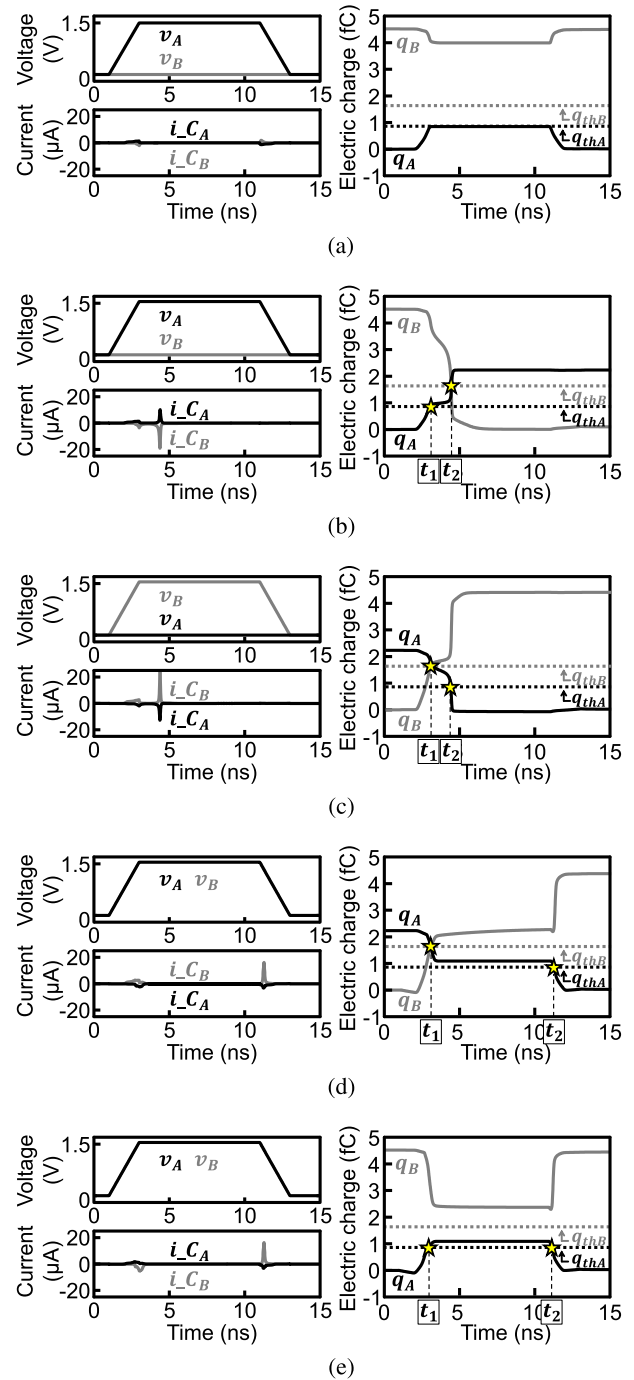


Fig. 5. Waveform of the bit-flip circuit simulation. (a) Cond. 1 ($V_{pA} = 1.5$ V, $V_{pB} = 0$ V, $Q_{ini} = "0"$). (b) Cond. 2 ($V_{pA} = 1.55$ V, $V_{pB} = 0$ V, $Q_{ini} = "0"$). (c) Cond. 3 ($V_{pA} = 0$ V, $V_{pB} = 1.55$ V, $Q_{ini} = "1"$). (d) Cond. 4 ($V_{pA} = 1.55$ V, $V_{pB} = 1.55$ V, $Q_{ini} = "1"$). (e) Cond. 5 ($V_{pA} = 1.55$ V, $V_{pB} = 1.55$ V, $Q_{ini} = "0"$).

because C_B contains additional fan-in capacitances, q_A reaches the threshold value q_{thA} first. Consequently, the NAND switches to a high-output state and fully charges q_B . This behavior is caused by the large gate capacitance of INV2, which is supposed to drive the next cell stage, resulting in C_B being larger than C_A . For the standard cells, we discuss from Section IV, all D-FF cells have this high C_B . Therefore, a "bit-reset error" is likely to occur

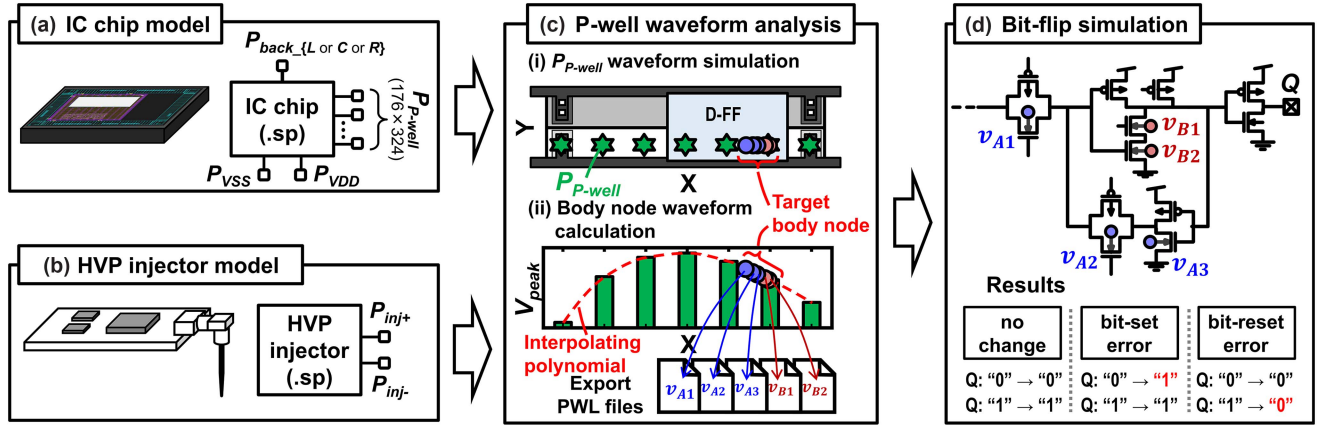


Fig. 6. Simulation flows of HVP injection on backside of ICs.

when the amplitude of v_A equals that of v_B in these standard cells.

This analysis shows that variations in body voltages can lead to bit-flips in bistable circuits. Moreover, even any small voltage difference among the body of transistors leads to a characteristic “bit-set error” or “bit-reset error.”

IV. FULL-CHIP MODEL AND SIMULATION

In this section, the bit-flip phenomenon in the static state of the D-FF due to the application of HVP on the backside of the IC is simulated using the proposed simulation flow of Fig. 6. First, RC models of the IC chip and the HVP injector are created to analyze the P-well voltage fluctuations. Based on these models, we perform transient analysis by using SPICE and draw intensity maps from the simulated P-well voltage waveforms. Voltage waveforms of the NMOS bodies of the D-FF shown in Fig. 3 are generated by interpolation using the coordinate information among D-FFs in the IC-chip level physical layout and the simulated P-well voltage waveforms selected for the nodes nearby each D-FF cell. The obtained waveforms are given to the bit-flip simulation. We will assess the bit-flip response of D-FF cells to the P-well voltage variation induced by the HVP on IC backside, with the function of its intensity as well as the relative location against the physical layout of IC frontside, in the following sections.

A. IC Chip Model

We define analysis ports for simulation over the IC chip given in Fig. 7, such as the injection ports (P_{back_L} , P_{back_C} , and P_{back_R}) on the backside of the Si substrate, the PDN ports (P_{VDD} , P_{VSS}) given on respective metal pads and the voltage measurement ports (P_{P-well}) distributed in the P-well region.

The chip [see Fig. 7(a)] was prototyped with a CMOS twin-well bulk transistor technology. The die size of the chip is $4\text{ mm} \times 3\text{ mm}$. The power mesh, which supplies all digital ICs with cryptographic functionality, takes up most of the chip area. In this study, the register file of 720 D-FF cells, in a control part of the cryptographic engine and within the area of approximately $1300\text{ }\mu\text{m} \times 500\text{ }\mu\text{m}$ are selected for evaluation. As shown in

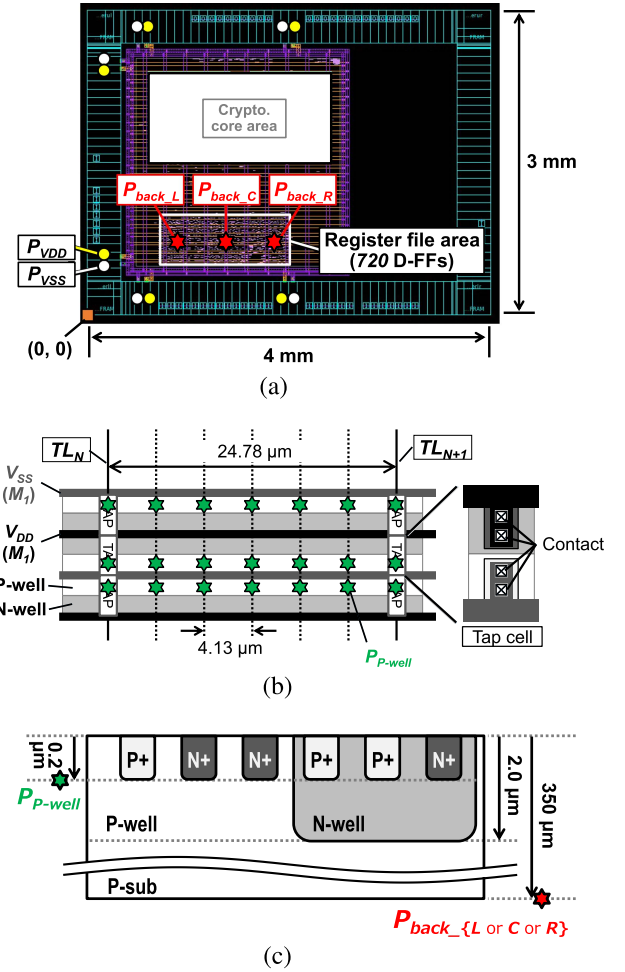


Fig. 7. Port arrangement in the IC model. (a) Top view. (b) Detailed view in the register file area. (c) Side view.

Fig. 7(a), to assess the positional dependency of the HVP on the IC backside, three voltage injection ports named P_{back_L} , P_{back_C} , and P_{back_R} are positioned with an interval of $500\text{ }\mu\text{m}$ from each other. As can be seen in Fig. 7(b), the tap cells have the important function of connecting P-well and N-well via contacts

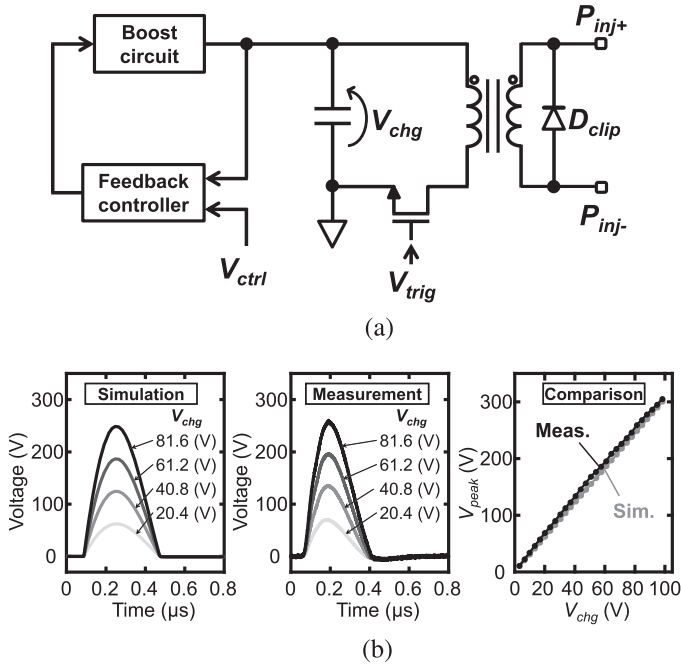


Fig. 8. Schematic of the HVP injector. (a) Schematic of the HVP injector. (b) Evaluation of the HVP injector model.

with V_{SS} and V_{DD} , respectively, thus ensuring that the correct bias voltage is maintained. The tap line (TL) is defined as a vertical line with the tap cells and regularly placed at the horizontal interval of $24.78 \mu m$.

As shown in Fig. 7(b) and Fig. (c), the P_{P-well} positions for measuring the P-well voltage are placed at the intervals of $4.13 \mu m$, dividing between the two TLs into six parts. The depth of the P_{P-well} layer is $0.2 \mu m$, which is the same height of the highly doped regions of P+ and N+. There are $176 \times 324 P_{P-well}$ positions in each of the vertical and horizontal directions in the register file area. The thickness of the Si substrate is $350 \mu m$.

The RC circuit model of the IC chip is extracted among the analysis ports. The resistivity of substrate layers and the capacitance between each substrate layer are extracted from experimental measurements, while the resistivity of metallic (Cu and Al) wires is calculated from the numbers in physical design kit from the IC manufacturer.

B. HVP Injector Model

Fig. 8(a) shows the HVP injector circuit supplying voltage pulses to the backside of the ICs. The amplitude can be controlled by the precharge voltage V_{chg} , which appears on the capacitor as a charge reservoir and is finely regulated by the feedback loop depending on the external control voltage V_{ctrl} . The charge is released by the trigger signal V_{trig} to excite a current on the secondary side of the transformer. The diode D_{clip} is used to prevent bouncing due to the reflections between the HVP injector and the target load. The performance characteristics of the voltage waveform during injection are shown in Fig. 8(b), when a load resistor of 50Ω is intentionally inserted between P_{inj+} and P_{inj-} of the HVP injector. We confirmed the almost

linear increase of V_{peak} against V_{chg} and the expected agreements between measurement and simulation. It is of importance to note for our experiments that the injector exhibits a superior time synchronization performance than an ESD gun, since the triggering structure is made of transistors in the former, in contrast to a mechanical relay switch in the latter.

C. P-Well Waveform Analysis

The chip-level computation of the body voltage in bit-flip occurrences consists of two steps. First, P_{P-well} waveforms are calculated by simulating the transient response. Second, the interpolation is performed from the peak voltage of P_{P-well} waveforms to calculate the body voltage. This two-step approach eliminates the need of full grained meshing of an entire IC chip at the transistor-level, while allows the analysis ports to be assigned sparsely, heuristically, and empirically on the IC layout of interest. The computation time is then greatly suppressed.

The IC chip model and the HVP injector model are combined for the transient analysis. To evaluate the response to a positive HVP injection, we select the analysis ports to be properly connected in a way as P_{inj+} of the HVP injector to P_{back} of the IC chip model and P_{inj-} of the HVP injector to P_{VSS} of the IC chip model. Fig. 9 shows voltage intensity maps constructed from the peak points of the voltage waveforms of P_{P-well} s resulting from the transient simulation performed for the case of V_{chg} of 45 V. It is exhibited that the distribution is strongly localized around the position of IC backside injection. We also see that the voltage difference varies depending on the distance of the point from TLs.

To evaluate bit-flip errors, the voltages of the NMOS body coordinates of the D-FF are calculated from the voltage waveforms of P_{P-well} . The body voltages v_{A1} , v_{A2} , v_{A3} , v_{B1} , and v_{B2} are calculated from the neighboring P_{P-well} peak points using the piecewise cubic hermite interpolating polynomial. Then, a circuit-level bit-flip simulation in Section III is performed using the respective body voltage waveforms represented in a piecewise linear (PWL) format.

D. Bit-Flip Simulation

Fig. 10 shows bit-flip simulation results with the PWL files obtained from the P_{P-well} waveforms within the register file area. In accordance with the voltage intensity maps in Fig. 9, it can be seen that bit-flip errors occur strongly depending on the injection point. A key aspect of these results is that not all of the bits are inverted even in the proximity to the points of injection. According to the results in Fig. 3, it is assumed that this depends on the size of v_{A1} , v_{A2} , v_{A3} , v_{B1} , and v_{B2} and the stored data of the D-FF. In other words, bit-flip errors due to HVP from the backside of the IC are characterized by the initial state of Q and the placement of the D-FF relative to the position of the tap cells. This finally incurs bit-set or bit-reset errors. The analysis will be detailed in Section V and compared with measured results.

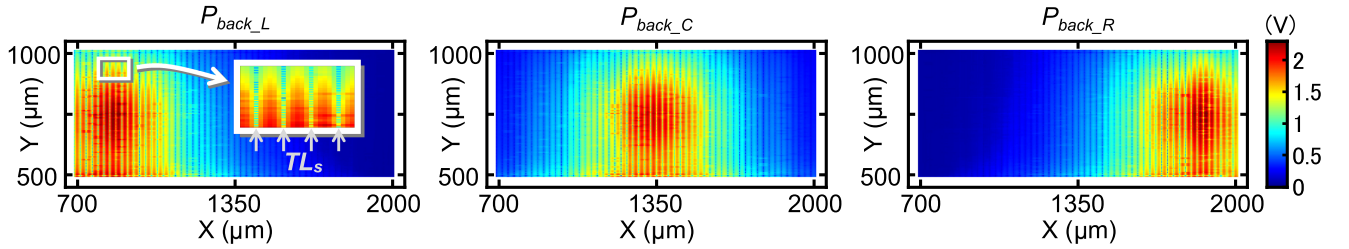


Fig. 9. P-well voltage intensity maps induced by HVP injection.

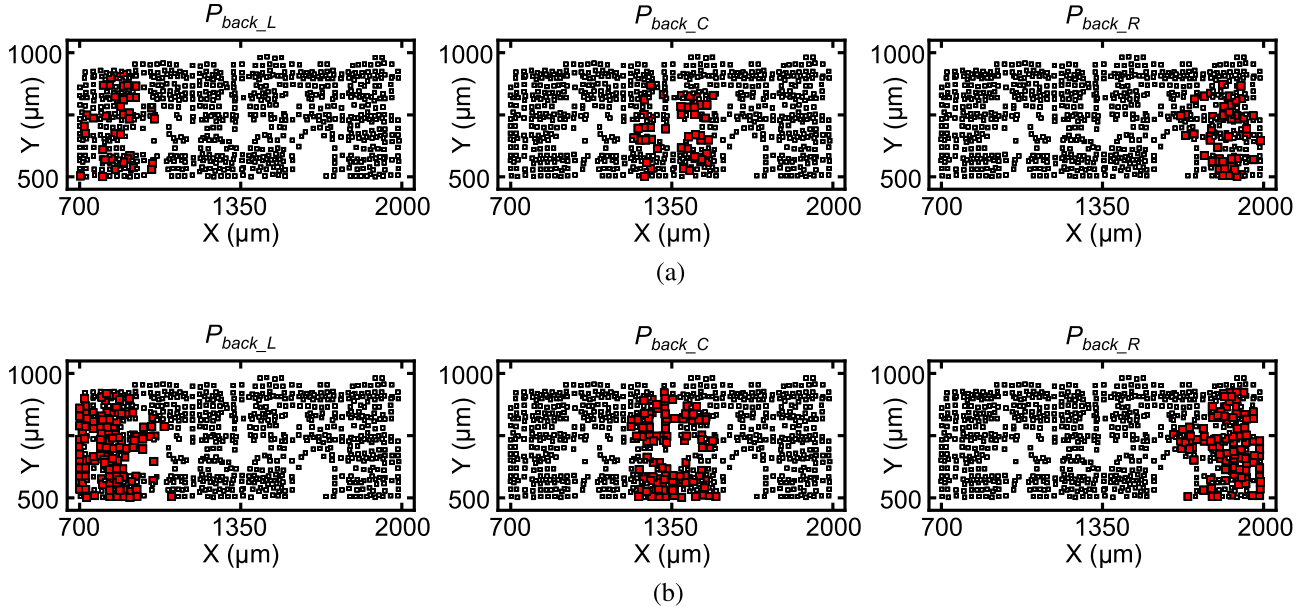


Fig. 10. Layout-dependent bit-flip errors in simulation. (a) Bit-set error. (b) Bit-reset error.

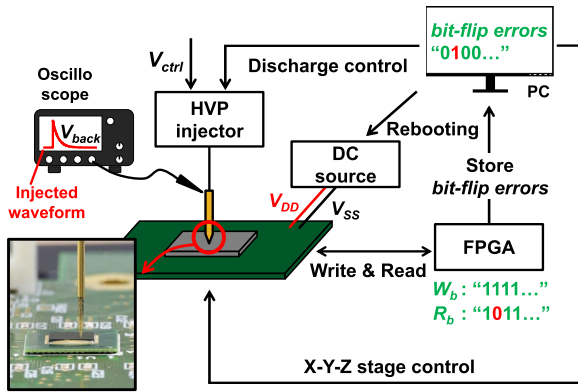


Fig. 11. Experiment setup of HVP injection on backside of ICs.

V. EXPERIMENTS

A. Measurement Setup

We experimentally observe the bit-flip errors in the static state of the bistable circuit by applying a positive HVP injection on the backside of the IC [13]. The experimental setup is shown in Fig. 11. The prototype chip [see Fig. 7(a)] was consisted of twin-well bulk CMOS transistors and back and thinned with $350\ \mu\text{m}$

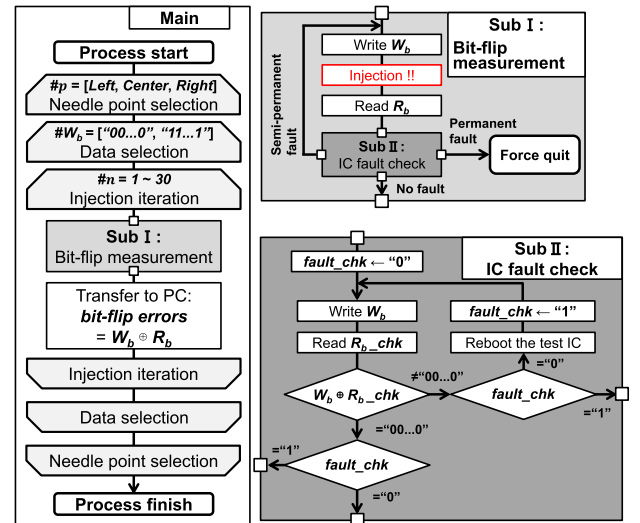


Fig. 12. Experimental flow diagram for bit-flip error evaluation.

in thickness after Si backgrinding. The IC chip is mounted in a flip-chip system on an evaluation board. The binary digital numbers among 720 D-FFs in the register file area are written

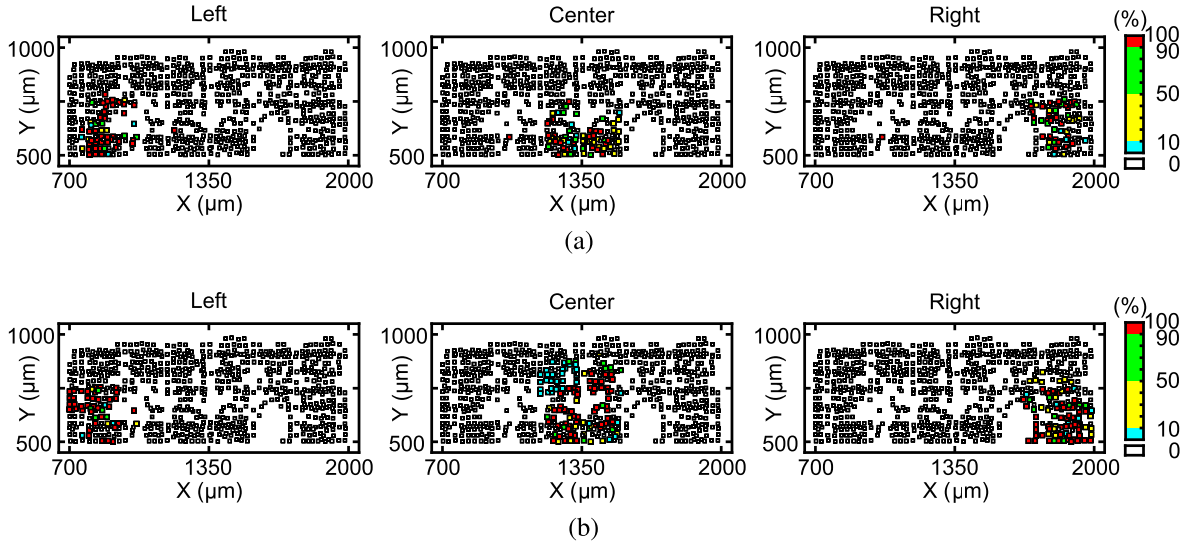


Fig. 13. Layout-dependent bit-flip errors in experiment. (a) Bit-set error. (b) Bit-reset error.

and read by a field programmable gate array (FPGA) in the setup. In Fig. 8(a), P_{inj+} contacts the Si backside with a needle. The tip of the injection needle has a spring mechanism that prevents the chip from being shaved or cracked by unexpectedly strong pressure on the backside of the ICs. The thin tip of the needle also precisely focuses on the point of interest on the back of the register file area. An automatic X - Y - Z stage with a resolution accuracy of $2\ \mu\text{m}$ in the XY direction and $1\ \mu\text{m}$ in the Z -direction, respectively, is remotely manipulated by an external controller (PC). This setup assures to improve the positioning accuracy of the needle and the uniform pressure of its tapping on the IC backside. During the positioning process, the needle first scans the four corners of the chip with the automatic stage and calculates a correction value for the axis misalignment between the stage and the IC chip. The needle tip then moves based on the layout information and the correction value to accurately target the test point in the register file area. P_{inj-} is connected to the V_{SS} via an evaluation board. An active probe with the high-voltage ($< 800\ \text{V}$) tolerance captures the backside pulse waveform V_{back} with an oscilloscope.

B. Bit-Flip Measurements

Fig. 12 shows the flowchart of the bit-flip error evaluation. The main part of the flowchart is responsible for controlling the measurement parameters. Sub I executes the bit-flip measurements. After the bit sequence W_b is written to the register file on the IC, HVP injection is applied. The bit sequence R_b is read out from the register file and stored in the FPGA with the associated address information. No clock signal is supplied to the D-FFs during injection and the value is latched in the follower. Sub II confirms that bit-flip errors are not semipermanent fault like latch-up of IC chips or even permanent due to transistor degradation. If the exclusive OR (XOR) operation among 720-b sequence between the newly written bit sequences W_b and the read bit sequences R_{b_chk} without injection wrongly asserts

any bit of 1, the setup forces the chip to be rebooted. The XOR sequence is then looped for classifying whether it is semipermanent or permanent, and the setup will terminate if the loop count continuously increases (assuming it is almost permanent). If there is no fault in the setup through Sub II loops, the bit-flip errors determined by the XOR operation between W_b and R_b are recorded in the PC with associated address information.

We conducted an experiment to investigate the injection position dependency by using an X - Y - Z stage to contact the needle at three locations ($\#p = [\text{Left}, \text{Center}, \text{Right}]$) at $500\ \mu\text{m}$ intervals. Furthermore, to evaluate the response according to the data stored in the D-FF, bit-set errors ($\#W_b = "00..0"$) or bit-reset errors ($\#W_b = "11..1"$) are measured. This experiment is repeated 30 times ($\#n$) at each $\#p$ and $\#W_b$ for statistically reliable results.

In the following experiments, V_{ctrl} is set to $1.6\ \text{V}$ and the bit-flip error of D-FF in the register file area is analyzed. The precharge voltage V_{chg} of the charging capacitor of the HVP injector is $54.4\ \text{V}$ and the peak of chip-backside voltage V_{back} is $428\ \text{V}$. Fig. 13 shows the results of the bit-set errors and bit-reset errors at each injection point on the layout coordinate plane. It can be seen that the errors are mainly concentrated at the injection point, while interestingly, the location of the bit-set errors and the bit-reset errors are not necessarily the same. This difference in the occurrence of bit-set and bit-reset errors suggests that the initial state of the bistable circuit and the placement with respect to the P-well contacts are surely relevant. In this experiment, there is no permanent fault of the evaluation IC during the measurement sequence in Fig. 12.

C. Comparison of Measurement Versus Simulation

We here newly introduce the S -axis ($-12.39\ \mu\text{m} \leq S < 12.39\ \mu\text{m}$) for evaluation as shown in Fig. 14 to confirm that bit-set errors and bit-reset errors are characterized by the D-FFs placement relative to the P-well contacts.

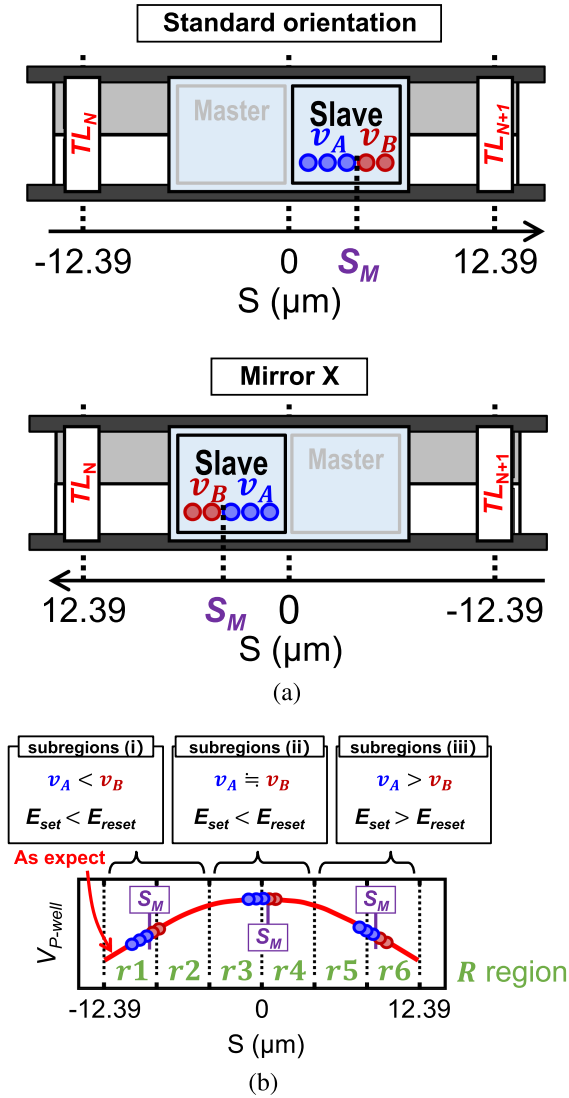


Fig. 14. Normalization of D-FF placement coordinates. (a) Standard cell arrangement. (b) Normalization of arrangement.

The alignment of D-FFs after a place and route (PnR) process is categorized into the standard orientation placement and mirror X placement based on the positional relationship between TLs and each body node, as shown in Fig. 14(a). The distance between TL_N and TL_{N+1} is $24.78 \mu\text{m}$, and the horizontal coordinate (S) of the body bias points for v_A is smaller than that for v_B . We also define S_M at the center between the coordinates for v_A and v_B . R region between TL_N and TL_{N+1} is divided into six subregions ($R \in \{r1, r2, r3, r4, r5, r6\}$) with an equal space on the axis of S , as shown in Fig. 14(b). The relation of body voltage and possible bit-flips are extracted in each region.

The formula for calculating the error rate in the six subregions in simulation and experiment is shown in (1), (2).

Bit-error rate equation for simulation

$$E_{\text{set_sim}}(r_{-i}) = \frac{\sum_{p=1}^3 (N_{\text{set_sim}}(r_{-i}, p))}{3 \times N_{\text{bits}}(r_{-i})}$$

$$E_{\text{reset_sim}}(r_{-i}) = \frac{\sum_{p=1}^3 (N_{\text{reset_sim}}(r_{-i}, p))}{3 \times N_{\text{bits}}(r_{-i})}. \quad (1)$$

Bit-error rate equation for experiment

$$E_{\text{set_exp}}(r_{-i}) = \frac{\sum_{n=1}^{30} \sum_{p=1}^3 (N_{\text{set_exp}}(r_{-i}, p, n))}{30 \times 3 \times N_{\text{bits}}(r_{-i})}$$

$$E_{\text{reset_exp}}(r_{-i}) = \frac{\sum_{n=1}^{30} \sum_{p=1}^3 (N_{\text{reset_exp}}(r_{-i}, p, n))}{30 \times 3 \times N_{\text{bits}}(r_{-i})} \quad (2)$$

where

p = needle point

n = injection iteration

r_{-i} = subregions of R region ($i = 1, 2, \dots, 6$)

Here, $N_{\text{bits}}(r_{-i})$ are the number of bits present in each subregion of R . The number of bit-set errors and bit-reset errors are defined as $N_{\text{set_sim}}(r_{-i})$ and $N_{\text{reset_sim}}(r_{-i})$ from the simulation results in Fig. 10 and $N_{\text{set_exp}}(r_{-i})$ and $N_{\text{reset_exp}}(r_{-i})$ from the measurement results in Fig. 13. The variable $\#p$ represents the three injection points. In the experiment, the results of 30 iterations by variable $\#n$ are averaged.

As shown in the P-well voltage simulation in Fig. 9, the P-well of the subregions $r1$ and $r6$, at both ends of R , indicate a low voltage because it is connected to the low-impedance metal V_{SS} wiring via P-well contacts. The R entirely exhibit the almost parabolic distribution of P-sub voltage among subregions, as expected in Fig. 14(b). The results in Section III indicate that bit-flip errors are distinctively characterized in accordance with the physical location of S_M falling in the subregions of $\{r1, r2\}$, $\{r3, r4\}$, $\{r5, r6\}$, as follows in detail.

subregions (i): When S_M falls in the subregions $r1$ and $r2$, $v_A < v_B$. Therefore, more “bit-reset error”s are observed.

subregions (ii): When S_M falls in the subregions $r3$ and $r4$, $v_A = v_B$. As explained in detail in cond. 4 and 5 of Fig. 5, due to the large gate capacitance of the output INV2 in Fig. 3, $C_A < C_B$, “bit-reset error”s are more observed than “bit-set error”s.

subregions (iii): When S_M falls in the subregions $r5$ and $r6$, $v_A > v_B$. Therefore, more “bit-set error”s are observed.

The error rates for the six subregions within the R region obtained by simulation and experiment are compared in Fig. 15 and showing the consistency of trends. This naturally comes from the P-sub voltage distribution. The simulation also validates the explanation in Section II that the primary path of current induced by the positive HVP is formed through the NMOS body-drain and body-source diodes and incurs bit-flips in D-FF cells. This will help physical-level designers to properly insert and locate tap cells in PnR process before sign-off procedures. The deviation of bit-flip trends within the entire R region can be further clarified with more detailed models at the cost of computation.

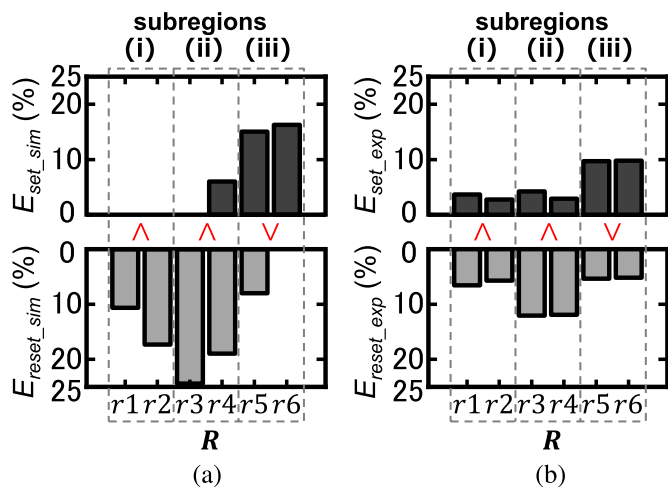


Fig. 15. Comparison of the bit-flip error rate between simulation and experiment. (a) Simulation. (b) Experiment.

VI. CONCLUSION

Focusing on an IEMI attack from the backside of the ICs, we devised a new current flow model for bit-flip in static-state bistable circuits. A positive current injected into a localized area on the backside of the ICs spreads through the Si substrate in three dimensions and flows to the PDN. This current flows through the P-well/N+ diode and charges the gate capacitance of the next stage. This phenomenon causes bit-flip errors in bistable circuits in the static state. The difference of resistivity among PDNs and P-wells leads to the voltage distribution in a region bounded by tap cells at both ends, and the occurrence of bit errors varies depending on the transistor placement and stored data. A model to represent these factors is constructed from IC chip design data, and simulations are performed. Experiments are also conducted on a prototype chip in flip-chip assembly to verify the validity of the simulation results. This research can be used to improving the backside voltage tolerance of specific bits without additional processes and to introduce circuit-level countermeasures using for instance canary circuits in IEMI, and is expected to contribute to semiconductor designs that require high reliability and confidentiality.

REFERENCES

- [1] W. Radasky, C. Baum, and M. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)," *IEEE Trans. Electromagn. Compat.*, vol. 46, no. 3, pp. 314–321, Aug. 2004.
- [2] D. Nitsch, M. Camp, F. Sabath, J. T. Haseborg, and H. Garbe, "Susceptibility of some electronic equipment to HPEM threats," *IEEE Trans. Electromagn. Compat.*, vol. 46, no. 3, pp. 380–389, Aug. 2004.
- [3] Y.-I. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, "Transient IEMI threats for cryptographic devices," *IEEE Trans. Electromagn. Compat.*, vol. 55, no. 1, pp. 140–148, Feb. 2013.
- [4] F. Sabath, "A systematic approach for electromagnetic interference risk management," *IEEE Electromagn. Compat. Mag.*, vol. 6, no. 4, pp. 99–106, Fourth Quarter 2017.
- [5] *Electromagnetic Compatibility (EMC)—Part 4-2: Testing and Measurement Techniques—Electrostatic Discharge Immunity Test*, IEC Standard 61000-4-2 Ed 2.0, 2008.

- [6] *Integrated Circuits—EMC Evaluation of Transceivers—Part 3: CAN Transceivers*, IEC Standard 62228-3:2019, 2019.
- [7] *Electromagnetic Compatibility (EMC)—Part 6-1: Generic Standards—Immunity for Residential, Commercial and Light-Industrial Environments*, IEC Standard 61000-6-1, 2016.
- [8] R. Nabhan, J.-M. Dutertre, J.-B. Rigaud, J.-L. Danger, and L. Sauvage, "A tale of two models: Discussing the timing and sampling EM fault injection models," in *Proc. Workshop Fault Detection Tolerance Cryptogr.*, 2023, pp. 1–12.
- [9] S. Ordas, L. Guillaume-Sage, and P. Maurine, "Electromagnetic fault injection: The curse of flip-flops," *J. Cryptographic Eng.*, vol. 7, no. 3, pp. 183–197, 2017.
- [10] C. O'Flynn, "Short paper: EMFI for safety-critical testing of automotive systems," in *Proc. Workshop Fault Detection Tolerance Cryptogr.*, 2021, pp. 61–66.
- [11] R. Hasegawa, K. Monta, T. Wadatsumi, T. Miki, and M. Nagata, "On-chip evaluation of voltage drops and fault occurrence induced by Si backside EM injection," in *Constructive Side-Channel Analysis and Secure Design*, R. Wacquez and N. Homma, Eds. Cham, Switzerland: Springer, 2024, pp. 22–37.
- [12] T. Wadatsumi et al., "Voltage surges by backside ESD impacts on IC chip in flip chip packaging," in *Proc. IEEE Int. Rel. Phys. Symp.*, 2022, pp. P14-1–P14-6.
- [13] T. Wadatsumi, K. Kawai, R. Hasegawa, K. Monta, T. Miki, and M. Nagata, "Characterization of backside ESD impacts on integrated circuits," in *Proc. IEEE Int. Rel. Phys. Symp.*, 2023, pp. 1–6.
- [14] P. Maurine, K. Tobich, T. Ordas, and P. Y. Liardet, "Yet another fault injection technique : By forward body biasing injection," in *Proc. Yet Another Conf. Cryptogr.*, Porquerolles Island, France, Sep. 2012.
- [15] G. Chancel, J.-M. Galliere, and P. Maurine, "Body biasing injection: To thin or not to thin the substrate?," in *Constructive Side-Channel Analysis and Secure Design*, J. Balasch and C. O'Flynn, Eds. Cham, Switzerland: Springer, 2022, pp. 125–139.
- [16] O. A. Amusan et al., "Charge collection and charge sharing in a 130nm CMOS technology," *IEEE Trans. Nucl. Sci.*, vol. 53, no. 6, pp. 3253–3258, Dec. 2006.
- [17] J. D. Black, P. E. Dodd, and K. M. Warren, "Physics of multiple-node charge collection and impacts on single-event characterization and soft error rate prediction," *IEEE Trans. Nucl. Sci.*, vol. 60, no. 3, pp. 1836–1851, Jun. 2013.
- [18] J. Furuta, R. Yamamoto, K. Kobayashi, and H. Onodera, "Evaluation of parasitic bipolar effects on neutron-induced SET rates for logic gates," in *Proc. IEEE Int. Rel. Phys. Symp.*, 2012, pp. SE.5.1–SE.5.5.
- [19] N. Monnerau, F. Caignet, N. Nohier, M. Bafleur, and D. Tremouilles, "Investigation of modeling system ESD failure and probability using IBIS ESD models," *IEEE Trans. Device Mater. Rel.*, vol. 12, no. 4, pp. 599–606, Dec. 2012.
- [20] M. Park et al., "Measurement and analysis of statistical IC operation errors in a memory module due to system-level ESD noise," *IEEE Trans. Electromagn. Compat.*, vol. 61, no. 1, pp. 29–39, Feb. 2019.
- [21] M. Jeong, M. Shin, J. Kim, M. Seung, S. Lee, and J. Kim, "Measurement and analysis of system-level ESD-Induced jitter in a delay-locked loop," *IEEE Trans. Electromagn. Compat.*, vol. 62, no. 5, pp. 1840–1851, Oct. 2020.
- [22] L. Yang, C. Yang, Y. Tu, X. Wang, and Q. Wang, "Field-circuit co-simulation method for electrostatic discharge investigation in electronic products," *IEEE Access*, vol. 9, pp. 33512–33521, 2021.
- [23] L. Zussa, J.-M. Dutertre, J. Clediere, and B. Robisson, "Analysis of the fault injection mechanism related to negative and positive power supply glitches using an on-chip voltmeter," in *Proc. IEEE Int. Symp. Hardware-Oriented Secur. Trust*, 2014, pp. 130–135.



Takuya Wadatsumi (Student Member, IEEE) received the B.S. and M.S. degrees in engineering in 2019 and 2021, respectively, from Kobe University, Kobe, Japan, where he is currently working toward the doctoral degree in science, technology and innovation with the Graduate School of Science, Technology and Innovation.

His research mainly focuses on the area of semiconductor reliability, especially against electromagnetic compatibility and electrostatic discharge. His work contributes to the hardening of design techniques against these disturbances by developing advanced simulation techniques and countermeasures.



Kazuki Monta (Member, IEEE) received the B.S. degree in engineering and M.S. and Ph.D. degrees in science, technology and innovation from Kobe University, Kobe, Japan, in 2018, 2020, and 2024, respectively.

He is currently the President and a co-founder of Secafy Company Ltd., Kobe, Japan, while also a Scientific Researcher with Kobe University. His research primarily focuses on the domain of hardware security, specifically addressing critical issues, such as side-channel attacks and fault injection attacks. His work contributes to mitigate these threats by developing advanced simulation techniques and countermeasures.

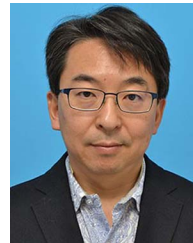


Adrijan Barić (Senior Member, IEEE) received the Dipl.-Ing. and M.Sc. degrees in electrical engineering from the University of Zagreb, Zagreb, Croatia, in 1982 and 1985, respectively, and the Ph.D. degree in electronics from Dublin City University, Dublin, Ireland, in 1995.

Since 1984, he has been with the University of Zagreb. His research interests include semiconductor device modeling, integrated circuit design, interconnect modeling, and electromagnetic compatibility.



Yusuke Hayashi received the B.S. degree in engineering in 2023 from Kobe University, Kobe, Japan, where he is currently working toward the master's degree in science, technology and innovation with the Graduate School of Science, Technology and Innovation.

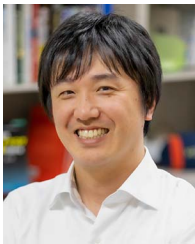


Makoto Nagata (Senior Member, IEEE) received the B.S. and M.S. degrees in physics from Gakushuin University, Tokyo, Japan, in 1991 and 1993, respectively, and the Ph.D. degree in electronics engineering from Hiroshima University, Hiroshima, Japan, in 2001.

He was a Research Associate with Hiroshima University from 1994 to 2002 and from 2002 to 2009, an Associate Professor with Kobe University, Kobe, Japan, where he was promoted to a Full Professor in 2009. His research interests include design techniques

targeting high-performance mixed analog, RF and digital VLSI systems with particular emphasis on power/signal/substrate integrity and electromagnetic compatibility, testing and diagnosis, three-dimensional system integration, as well as their applications for hardware security and safety, and cryogenic electronics for quantum computing.

Dr. Nagata is a Senior Member of IEICE. He has been a member of a variety of technical program committees of international conferences, such as the Symposium on Very Large Scale Integration (VLSI) Circuits (2002–2009), Custom Integrated Circuits Conference (2007–2009), Asian Solid-State Circuits Conference (2005–2009), International Solid-State Circuits Conference (2014–2022), European Solid-State Circuits Conference (since 2020), and many others. He chaired the Technology Directions subcommittee for International Solid-State Circuits Conference (2018–2022) and served for an Executive Committee Member (since 2023). He was the Technical Program Chair (2010–2011), the Symposium Chair (2012–2013), and an Executive Committee Member (2014–2015) for the Symposium on VLSI circuits. He was the IEEE Solid-State Circuits Society (SSCS) AdCom member (2020–2022), the distinguished Lecturer (2020–2021, and since 2024), and currently the chapters Vice Chair (since 2022) of the society. He is currently an Associate Editor for IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION SYSTEMS (since 2015).



Takuji Miki (Member, IEEE) received the Ph.D. degree in electrical engineering from Kobe University, Kobe, Japan, in 2017.

From 2006 to 2017, he was with Panasonic Corporation, Osaka, Japan, where he was involved in the development of analog and mixed-signal integrated circuits for consumer and industrial applications. He is currently an Associate Professor with the Graduate School of Science, Technology and Innovation, Kobe University. His current research interests include data converters, hardware security, and cryogenic CMOS

circuits for quantum computers.

Dr. Miki is currently a member of technical program committees for the IEEE Asian Solid-State Circuits Conference and the IEEE European Solid-State Circuits Conference.



Alkis A. Hatzopoulos (Life Senior Member, IEEE) was born in Thessaloniki, Greece. He received the B.Sc degree in physics (with *hons.*), the master's degree in electronics, and the Ph.D. degree in electrical engineering from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1980, 1983, and 1989, respectively.

Since 1981, he has been with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, where he is currently a Professor and the Director of the Electronics Laboratory.

His research interests include modeling, design and fault diagnosis of integrated circuits and systems (analog, mixed-signal, high-frequency), electronic communication circuits, thin-film transistors, instrumentation electronics, space applications.

Dr. Hatzopoulos was a Chapter Chair for the IEEE Greek Chapter of Circuits and Systems and Solid-State Circuits for 10 years. He is actively involved in educational and research projects, and he is the author or coauthor of more than 180 scientific papers in international journals and conference proceedings.